Free Questions for II0-001 by vceexamstest

Shared by Stuart on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An active traceback detects active network connections to a host.

Options:

A- True

B- False

Answer:

A

Question 2

Question Type: MultipleChoice

The following are components of an IP Datagram header except:

Options:

A- Type of Service

B- Total Length

C- Header Checksum

D- Default Gateway address

Answer:

D

Question 3

Question Type: MultipleChoice

Which of th following keymappers are the most difficult to detect by the subject of the monitoring?

Options:

A- Hardware keymapper

B- StealthMap

C- ShadowCopy

D- NSA's HAL9000.09 Signaling Mirror

Answer:

A

Question 4

Question Type: MultipleChoice

Keymappers are illegal in the following States in the U.S.:

Options:

A- California

B- Maryland

C- Connecticut

D- None of the above

Answer:

D

Question 5

Question Type: MultipleChoice

When introduced to a crime scene as an investigator you need to:

Options:

A- Maintain a written log

B- Contact the public information officer immediately

C- Secure the crime scene

D- Use sound forensic processes

E- A, B, & C

F- A, C, & D

Answer:

F

Question 6

Question Type: MultipleChoice

A well documented chain of custody must include:

Options:

A- Who took it out of evidence

B- Who witnessed the collection of evidence

C- Who collected the evidence

D- A, B & C

E- A & C

F- B & C

Answer:

D

Question 7

Question Type: MultipleChoice

The four steps in evidence handling in the proper order are:

Options:

A- Preserve, Identify, Analyze, & Present

B- Preserve, Analyze, Identify, & Present

C- Preserve, Present, Identify, & Analyze

D- Identify, Preserve, Analyze, & Present

Answer:

D

Question 8

Question Type: MultipleChoice

The best type of evidence to have would be:

Options:

A- Hearsay evidence

B- Conclusive evidence

C- Secondary evidence

D- Direct evidence

E- Primary evidence

Answer:

E

Question 9

Question Type: **MultipleChoice**

BCP consists of:

Options:

A- Malicious attack response

B- Crisis mitigation

C- Steps to take before and after an event

D- A, B & C

E- A & C

F- B & C

Answer:

E

Question 10

Question Type: **MultipleChoice**

A well rounded information security program should include:

Options:

A- Understanding on how to prevent events

B- A security awareness program

C- Understanding on how viruses work

D- All of the above

Answer:

B